

(19) 日本国特許庁 (J P)

(12) 公表特許公報(A)

(11)特許出願公表番号  
特表2002-514326  
(P2002-514326A)

(43)公表日 平成14年5月14日(2002.5.14)

(51) Int.Cl.<sup>7</sup> 識別記号  
G 0 6 F 11/00  
13/00 5 3 0

F I  
G 0 6 F 13/00 5 3 0 A  
9/06 6 6 0 N

テマコト（参考）

審查請求 未請求 予備審查請求 有 (全 38 頁)

(21)出願番号	特願平10-522345
(86) (22)出願日	平成9年11月6日(1997.11.6)
(85)翻訳文提出日	平成11年5月8日(1999.5.8)
(86)国際出願番号	PCT/IB97/01626
(87)国際公開番号	WO98/21683
(87)国際公開日	平成10年5月22日(1998.5.22)
(31)優先権主張番号	60/030, 639
(32)優先日	平成8年11月8日(1996.11.8)
(33)優先権主張国	米国(US)
(31)優先権主張番号	08/964, 388
(32)優先日	平成9年11月6日(1997.11.6)
(33)優先権主張国	米国(US)

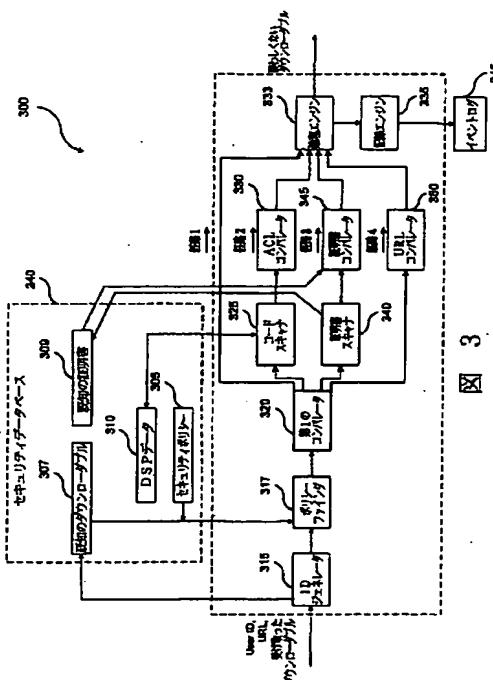
(71)出願人 フィンジャン ソフトウェア, リミテッド  
イスラエル国, 42945 ケファー・ハイム  
(72)発明者 トウボウル, シュロモ  
イスラエル国, 42945 ケファー・ハイム  
(74)代理人 弁理士 飯塚 義仁

最終頁に續く

(54) 【発明の名称】 悪意のあるダウンローダブルからコンピュータおよびネットワークを保護するためのシステムおよび方法

(57) [要約]

システムは、疑わしいダウンローダブルからコンピュータを保護する。このシステムは、セキュリティポリシーと、ダウンローダブルを受け取るためのインターフェイスと、このインターフェイスに接続されていて、前記セキュリティポリシーを前記ダウンローダブルに適用して、前記セキュリティポリシーが侵害されたか否かを判定するためのコンバレータとを備えている。前記ダウンローダブルは、Java(商標)アプレット、ActiveX(商標)コントロール、JavaScript(商標)スクリプト、または、Visual Basicスクリプトを含んでいてよい。前記セキュリティポリシーは、前記ダウンローダブルの宛先であるクライアントに問わらず適用されるデフォルトセキュリティポリシー、前記クライアントまたは該クライアントが属するグループに基づいて適用される特定のセキュリティポリシー、または、前記クライアント／グループおよび受け取った特定のダウンローダブルに基づいて適用される特定のセキュリティポリシーを含んでいてよい。このシステムは、好ましくは、前記ダウンローダブルのすべての構成要素をフェッチし、このフェッチした



**【特許請求の範囲】**

1. ダウンローダブルを受け取るステップと、

前記ダウンローダブルをセキュリティポリシーと比較し、前記セキュリティポリシーが侵害されたか否かを判定するステップと、

前記セキュリティポリシーが侵害された場合、前記ダウンローダブルを放棄するステップと

を具備するコンピュータに基づく方法。

2. 前記ダウンローダブルをダウンローダブルセキュリティファイルに分解するステップと、該ダウンローダブルセキュリティファイルを前記セキュリティポリシーと比較するステップとをさらに具備した請求の範囲第1項に記載の方法。

3. 証明書をスキャンし、該証明書を信頼性が確認された証明書と比較するステップをさらに具備した請求の範囲第1項に記載の方法。

4. 前記ダウンローダブルの送り元のURLを既知のURLと比較するステップをさらに具備した請求の範囲第1項に記載の方法。

5. 前記既知のURLが信頼性が確認されたURLである請求の範囲第4項に記載の方法。

6. 前記既知のURLが信頼性が確認されていないURLである請求の範囲第4項に記載の方法。

7. 前記ダウンローダブルがJava (商標) アプレットを含む請求の範囲第1項に記載の方法。

8. 前記ダウンローダブルがActiveX (商標) コントロールを含む請求の範囲第

1項に記載の方法。

9. 前記ダウンローダブルがJavaScript (商標) スクリプトを含む請求の範囲第1項に記載の方法。

10. 前記ダウンローダブルがVisual Basicスクリプトを含む請求の範囲第1項に記載の方法。

11. 前記ダウンローダブルの宛先がクライアントであり、前記セキュリティポリシーは、前記ダウンローダブルの宛先であるクライアントにかかるわらず適用さ

れるデフォルトセキュリティポリシーを含む請求の範囲第1項に記載の方法。

12. 前記ダウンローダブルの宛先がクライアントであり、前記セキュリティポリシーは、前記ダウンローダブルの宛先がクライアントである場合に適用される特定のセキュリティポリシーを含む請求の範囲第1項に記載の方法。

13. 前記ダウンローダブルの宛先がグループに属するクライアントであり、前記セキュリティポリシーは、前記クライアントが特定のグループに属する場合に適用される特定のセキュリティポリシーを含む請求の範囲第1項に記載の方法。

14. 前記ダウンローダブルの宛先がクライアントであり、前記ダウンローダブルを放棄した後に、その代替となる悪意の無いダウンローダブルを前記クライアントに送って通知するステップをさらに具備した請求の範囲第1項に記載の方法。

15. 前記ダウンローダブルを放棄した後に、前記侵害をイベントログに記録するステップをさらに具備した請求の範囲第1項に記載の方法。

16. 前記ダウンローダブルを識別するためのダウンローダブルIDを算出するステップをさらに具備した請求の範囲第1項に記載の方法。

17. 前記ダウンローダブルによって特定される構成要素をフェッチし、該フェッチされた構成要素を前記ダウンローダブルに含めるステップをさらに具備した請求の範囲第16項に記載の方法。

18. 前記ダウンローダブルについてハッシング関数を実行するステップをさらに具備した請求の範囲第17項に記載の方法。

19. 前記ダウンローダブルによって特定されるすべての構成要素をフェッチするステップをさらに具備した請求の範囲第17項に記載の方法。

20. 意図された受領者のユーザIDを検査し、適当なセキュリティポリシーを決定するステップをさらに具備した請求の範囲第1項に記載の方法。

21. 前記ダウンローダブルを検査し、適当なセキュリティポリシーを決定するステップをさらに具備した請求の範囲第1項に記載の方法。

22. 前記適当なセキュリティポリシーが、デフォルトセキュリティポリシーを含む請求の範囲第20項に記載の方法。

23. 前に受け取ったダウンローダブルを既知のダウンローダブルとして含める  
ステップをさらに具備した請求の範囲第26項に記載の方法。

24. 前記セキュリティポリシーが、管理オーバーライドごとに拒絶すべきダウ  
ンローダブルを指示する請求の範囲第23項に記載の方法。

25. 前記セキュリティポリシーが、管理オーバーライドごとに許可すべきダウ  
ンローダブルを指示する請求の範囲第23項に記載の方法。

26. 前記ダウンローダブルを既知のダウンローダブルと比較するステップをさ  
らに具備した請求の範囲第1項に記載の方法。

27. 前記既知のダウンローダブルが悪意のあるものである請求の範囲第26項  
に記載の方法。

28. 前記既知のダウンローダブルが悪意の無いものである請求の範囲第26項  
に記載の方法。

29. 前記セキュリティポリシーがアクセスコントロールリストを含み、前記ダ  
ウンローダブルのセキュリティプロファイルデータを前記アクセスコントロール  
リストと比較するステップをさらに具備した請求の範囲第2項に記載の方法。

30. セキュリティポリシーの侵害を検出したときに、ユーザに通知するステッ  
プをさらに具備した請求の範囲第1項に記載の方法。

31. セキュリティポリシーと、  
ダウンローダブルを受け取るためのインターフェイスと、  
前記インターフェイスに接続されていて、前記セキュリティポリシーを前記ダ  
ウンローダブルに適用して、前記セキュリティポリシーが侵害されたか否かを判  
定するコンパレータと  
を具備したシステム。

32. 前記ダウンローダブルがJava（商標）アプレットを含む請求の範囲第31  
項に記載のシステム。

33. 前記ダウンローダブルがActiveX（商標）コントロールを含む請求の範囲  
第31項に記載のシステム。

3 4. 前記ダウンローダブルがJavaScript（商標）スクリプトを含む請求の範囲

第31項に記載のシステム。

3 5. 前記ダウンローダブルがVisual Basicスクリプトを含む請求の範囲第31

項に記載のシステム。

3 6. 前記ダウンローダブルの宛先がクライアントであり、前記セキュリティポリシーは、前記ダウンローダブルの宛先であるクライアントにかかわらず適用されるデフォルトセキュリティポリシーを含む請求の範囲第31項に記載のシステム。

3 7. 前記ダウンローダブルの宛先がクライアントであり、前記セキュリティポリシーは、前記ダウンローダブルの宛先がクライアントである場合に適用される特定のセキュリティポリシーを含む請求の範囲第31項に記載のシステム。

3 8. 前記ダウンローダブルの宛先がグループに属するクライアントであり、前記セキュリティポリシーは、前記クライアントが特定のグループに属する場合に適用される特定のセキュリティポリシーを含む請求の範囲第31項に記載のシステム。

3 9. 前記インターフェイスに接続されていて、前記ダウンローダブルを割りするダウンローダブルIDを算出するためのIDジェネレータをさらに具備した請求の範囲第31項に記載のシステム。

4 0. 前記IDジェネレータが、前記ダウンローダブルのすべての構成要素を予めフェッチし、該すべての構成要素を使用して前記ダウンローダブルIDを算出する請求の範囲第39項に記載のシステム。

4 1. 前記IDジェネレータが、予めフェッチされた前記すべての構成要素のデジタルハッシュを算出する請求の範囲第40項に記載のシステム。

4 2. 前記セキュリティポリシーを見つけるためのポリシーファインダをさらに具備した請求の範囲第31項に記載のシステム。

4 3. 前記ポリシーファインダが、前記ユーザに基づいて前記セキュリティポリシーを見つける請求の範囲第42項に記載のシステム。

4 4. 前記ポリシーファインダが、前記ユーザおよびダウンローダブルに基づい

て前記セキュリティポリシーを見つける請求の範囲第42項に記載のシステム。

45. 前記ポリシーファインダが、前記デフォルトセキュリティポリシーを求める請求の範囲第42項に記載のシステム。

46. 前記コンパレータが、前記セキュリティポリシーを検査して、適用すべきテストを決定する請求の範囲第31項に記載のシステム。

47. 前記コンパレータが、前記ダウンローダブルを既知のダウンローダブルと比較する請求の範囲第46項に記載のシステム。

48. 前記既知のダウンローダブルが悪意のあるものである請求の範囲第47項に記載のシステム。

49. 前記既知のダウンローダブルが悪意の無いものである請求の範囲第47項に記載のシステム。

50. 前記セキュリティポリシーが、管理オーバーライドごとに拒絶すべきダウンローダブルを指示する請求の範囲第31項に記載のシステム。

51. 前記セキュリティポリシーが、管理オーバーライドごとに許可すべきダウンローダブルを指示する請求の範囲第31項に記載のシステム。

52. 前記ダウンローダブルの宛先がクライアントであり、前記コンパレータは、代替となる悪意の無いダウンローダブルを前記クライアントに送って通知する請求の範囲第31項に記載のシステム。

53. 前記コンパレータに接続されていて、前記ダウンローダブルをダウンローダブルセキュリティプロファイルデータに分解するコードスキャナをさらに具備した請求の範囲第31項に記載のシステム。

54. 前記コードスキャナに接続されていて、前記ダウンローダブルセキュリティプロファイルデータをアクセスコントロールリストと比較するACLコンパレータをさらに具備した請求の範囲第53項に記載のシステム。

55. 前記コンパレータに接続されていて、前記ダウンローダブルにおける証明書を検査する証明書スキャナをさらに具備した請求の範囲第31項に記載のシステム。

56. 前記証明書スキャナに接続されていて、前記証明書を信頼性が確認された

証明書と比較する証明書コンパレータをさらに具備した請求の範囲第 55 項に記載のシステム。

57. 前記コンパレータに接続されていて、前記ダウンローダブルの送り元の URL を既知の URL と比較する URL コンパレータをさらに具備した請求の範囲第 31 項に記載のシステム。

58. 前記既知の URL が信頼性が確認されていない URL である請求の範囲第 57 項に記載のシステム。

59. 前記既知の URL が信頼性が確認された URL である請求の範囲第 57 項に記載のシステム。

60. 前記比較の結果に応答するための論理エンジンをさらに具備した請求の範囲第 31 項に記載のシステム。

61. 前記論理エンジンが、前記セキュリティポリシーに従って応答する請求の範囲第 31 項に記載のシステム。

62. 前記コンパレータに接続されていて、その結果をイベントログに記録する記録エンジンをさらに具備した請求の範囲第 31 項に記載のシステム。

63. ダウンローダブルを受け取る手段と、  
前記ダウンローダブルをセキュリティポリシーと比較し、前記セキュリティポリシーが侵害されたか否かを判定する手段と、  
前記セキュリティポリシーが侵害された場合、前記ダウンローダブルを放棄する手段と

を具備したシステム。

64. ダウンローダブルを受け取るステップと、  
前記ダウンローダブルをセキュリティポリシーと比較し、前記セキュリティポリシーが侵害されたか否かを判定するステップと、  
前記セキュリティポリシーが侵害された場合、前記ダウンローダブルを放棄するステップと  
をコンピュータに実行させるためのプログラムコードを格納してなる、コンピュータにより読み取り可能な記憶媒体。

65. ダウンローダブルを識別するためのダウンローダブルIDを生成するため

のコンピュータに基づく方法であつて、

ダウンローダブルコードを選択するステップと、

選択された前記ダウンローダブルコードについての関数を実行し、ダウンロー  
ダブルIDを生成するステップと、

前記ダウンローダブルIDを記憶するステップと

を具備する方法。

66. 前記関数がハッシング関数を含む請求の範囲第65項に記載の方法。

67. 前記ダウンローダブルコードが、ダウンローダブルの構成要素に対する参  
照を含み、前記構成要素をフェッチするステップをさらに具備した請求の範囲第  
65項に記載の方法。

68. 前記構成要素が、前記ダウンローダブルコードによって参照される第1の  
構成要素を含む請求の範囲第67項に記載の方法。

69. 前記選択されたダウンローダブルコードが、前記ダウンローダブルに含ま  
れ且つ該ダウンローダブルによって識別されるコードのすべてを含む請求の範囲  
第65項に記載の方法。

70. 前記ダウンローダブルによって参照されるすべての構成要素をフェッチす  
るステップをさらに具備した請求の範囲第67項に記載の方法。

**【発明の詳細な説明】**

悪意のあるダウンローダブルからコンピュータおよびネットワークを保護するためのシステムおよび方法

**発明の背景****1. 発明の分野**

この発明は、コンピュータネットワークに関し、特に、悪意のあるダウンローダブルからコンピュータおよびネットワークを保護するためのシステムおよび方法に関する。

**2. 背景技術の説明**

現在のインターネットは、政府、大学、非営利団体および会社によって所有される10万個以上の個々のコンピュータネットワークの集合であり、加速度的に拡張している。インターネットは公開的なものであるので、該インターネットは、通常“ウィルス”と呼ばれる、多くのシステムに損害を与えたりこれらを破壊したりするアプリケーションプログラムの主要発生源となっている。

従って、プログラマたちは、このようなウィルスが個々のコンピュータおよびネットワークを攻撃することを阻止するためのコンピュータおよびコンピュータネットワークセキュリティシステムを設計し続けている。ほとんどの場合、このようなセキュリティシステムは比較的成功している。しかしながら、これらのセキュリティシステムは、“ダウンローダブル(Downloadables)”と通称されているダウンロード可能なアプリケーションプログラムに付加され、または、ダウンロード可能なアプリケーションプログラムとして構成されたコンピュータビールスを認識できるよう構成されていない。前記ダウンローダブルとは、ソースコンピュータからダウンロードされ、送り先(デスティネーション)コンピュータ上で実行される実行可能なアプリケーションプログラムである。ダウンローダブルは、典型的には、インターネットブラウザまたはウェブエンジンなどを介して、進行中の処理によってリクエストされる。ダウンローダブルの例としては、Sun Microsystems, Inc. によって開発されたJava (商標) 配信環境での使用のために設計

されたJava（商標）アプレット、同じくSun Microsystems, Inc.によって開発されたJavaScriptスクリプト、Microsoft Corporationによって開発されたActiveX（商標）配信環境での使用のために設計されたActiveX（商標）コントロール、および、同じくMicrosoft Corporationによって開発されたVisual Basicが含まれる。従って、悪意のあるダウンローダブルからネットワークを保護するためのシステムおよび方法が必要となっている。

#### 発明の要点

この発明は、疑わしいダウンローダブルからネットワークを保護するためのシステムを提供する。該システムは、セキュリティポリシー（security policy）と、ダウンローダブルを受け取るためのインターフェイスと、該インターフェイスに接続されていて、前記セキュリティポリシーを前記ダウンローダブルに適用して、前記セキュリティポリシーが侵害されたか否かを判定するためのコンパレータとを具備している。前記ダウンローダブルは、Java（商標）アプレット、ActiveX（商標）コントロール、JavaScript（商標）スクリプト、または、Visual Basicスクリプトを含んでいてよい。前記セキュリティポリシーは、前記ダウンローダブルの宛先であるクライアントに関わらず適用されるデフォルトセキュリティポリシー、前記クライアントまたは該クライアントが属するグループに基づいて適用される特定のセキュリティポリシー、または、前記クライアント／グループおよび受け取った特定のダウンローダブルに基づいて適用される特定のセキュリティポリシーを含んでいてよい。該システムは、好ましくは、前記ダウンローダブルのすべての構成要素をフェッチし、該フェッチした構成要素を含むダウンローダブルについてハッシングファンクション（hashing function；ハッシング関数）を実行することによって、前記ダウンローダブルを識別するダウンローダブルＩＤを算出するためのＩＤジェネレータを使用する。

さらに、前記セキュリティポリシーは、（1）既知の悪意のあるダウンローダブルと悪意の無いダウンローダブルとの比較、（2）管理オーバーライドごとの拒絶または許可すべきダウンローダブルの比較、（3）ダウンローダブルセキュリティプロファイルデータの、アクセスコントロールリストに対する比較、（4）前記ダウンローダブルに含まれるサーティフィケート（certificate；証明又は

証明書；以下「証明書」という）の、信頼性が確認されたサーティフィケート（certificate；証明書）に対する比較、（5）前記ダウンローダブルの送り元のURLの、信頼性が確認されたURLおよび信頼性が確認されていないURLに対する比較、を含むいくつかの実行すべきテストを指示するものであってよい。

これらのテストに基づき、論理エンジンは、前記ダウンローダブルを許可または拒絶すべきことを判定することができる。

さらに、この発明は、疑わしきダウンローダブルからコンピュータを保護するための方法を提供する。この方法は、ダウンローダブルを受け取るステップと、前記ダウンローダブルをセキュリティポリシーと比較し、前記セキュリティポリシーが侵害されたか否かを判定するステップと、前記セキュリティポリシーが侵害されたか場合、前記ダウンローダブルを放棄するステップとを具備するものである。

この発明に係るシステムおよび方法は、既知の悪意のあるダウンローダブルからコンピュータを保護するものであってよい。この発明に係るシステムおよび方法は、疑わしいと判断されるオペレーションを実行するダウンローダブルを識別することができる。該システムおよび方法は、前記ダウンローダブルのコードを検査して、該コードが疑わしいオペレーションを含むか否かを判定し、この判定に応じて前記ダウンローダブルを許可または拒絶するものとすることができる。

#### 図面の簡単な説明

図1は、この発明に係るネットワークシステムを示すブロック図。

図2は、図1の内部ネットワークセキュリティシステムの詳細を示すブロック図。

図3は、図2のセキュリティプログラムおよびセキュリティデータベースの詳細を示すブロック図。

図4は、図3のセキュリティポリシーの詳細を示すブロック図。

図5は、図1のセキュリティ管理コンソールの詳細を示すブロック図

図6Aは、この発明に従って、疑わしいダウンローダブルの検査を行うための方法を示すフローチャート。

図 6 B は、図 6 A の適当なセキュリティポリシーを見つけるためのステップの詳細を示すフローチャート。

図 6 C は、入ってくるダウンローダブルを疑わしき物と判断すべきか否かを判定するための方法を示すフローチャート。

図 7 は、図 6 におけるダウンローダブルを分解するためのステップの詳細を示すフローチャート。

図 8 は、ダウンローダブルを識別するためのダウンローダブル ID を生成するための方法 800 を示すフローチャート。

#### 好ましい実施の形態の詳細な説明

図 1 は、この発明に係るネットワークシステム 100 を示すブロック図である。該ネットワークシステム 100 は、通信チャンネル 125 を介して内部ネットワークセキュリティシステム 110 に接続された、例えば、インターネットと通称されている広域ネットワーク (WAN) のような外部コンピュータネットワーク 105 を含んでいる。さらに、前記ネットワークシステム 100 は、通信チャンネル 130 を介して前記内部ネットワークセキュリティシステム 110 に接続され、且つ、通信チャンネル 135 を介してセキュリティ管理コンソール 120 に接続された、例えば、法人のローカルエリアネットワーク (LAN) のような内部コンピュータネットワーク 115 を含んでいる。

前記内部ネットワークセキュリティシステム 110 は、前記外部コンピュータネットワーク 105 から受け取ったダウンローダブルを検査し、疑わしいと思われるダウンローダブルが前記内部コンピュータネットワーク 115 に進入するのを阻止する。この場合、望ましくないオペレーションを行いもしくはその可能性のあるダウンローダブル、または、前記内部コンピュータネットワーク 115 の完全性に脅威を与えもしくはその可能性のあるダウンローダブルが疑わしいものと判断される。なお、“疑わしい”という用語は、悪意のある、潜在的に悪意のある、望ましくない、または、潜在的に望ましくない等々を意味する。前記セキュリティ管理コンソール 120 は、前記内部ネットワークセキュリティシステム 110 の目視確認、変更および環境設定を可能にする。

図2は、前記内部ネットワークセキュリティシステム110の詳細を示すプロック図である。該内部ネットワークセキュリティシステム110は、信号バス220に接続された、例えば、Intel Pentium(登録商標)マイクロプロセッサまたはMotorola Power PC(登録商標)のような中央処理ユニット(CPU)205を備えている。さらに、前記内部ネットワークセキュリティシステム110は、前記外部コンピュータネットワーク105からダウンローダブルを受け取るために前記通信チャネル125と信号バス220との間に接続された外部通信インターフェイス210と、疑わしいと思われないダウンローダブルを前記内部コンピュータネットワーク115に送るために前記信号バス220と前記通信チャネル130との間に接続された内部通信インターフェイス225とを備えている。前記外部通信インターフェイス210および内部通信インターフェイス225は、前記外部コンピュータネットワーク105からダウンローダブルを受け取る機能、および、ダウンローダブルを前記内部コンピュータネットワーク115に送るための機能を有する統合的な通信インターフェイス(図示せず)の機能要素であつてよい。

さらに、前記内部ネットワークセキュリティシステム110は、(キーボード、マウスおよびCRTディスプレイなどの)入／出力(I／O)インターフェイス215と、磁気ディスクなどのデータ記憶装置230と、ランダムアクセスメモリ(RAM)235とを備えており、これらの各々は前記信号バス220に接続されている。前記データ記憶装置230はセキュリティデータベース240を格納しており、該セキュリティデータベース240は、受け取ったダウンローダブルを疑わしいとすべきか否かを判定するためのセキュリティ情報を含んでいる。さらに、前記データ記憶装置230は、ダウンローダブルを受け取る可能性のある前記内部コンピュータネットワーク115内のユーザを示すユーザリスト260と、検査された各ダウンローダブルについての判定結果および前記内部ネットワークセキュリティシステム110の実行時表示を含むイベントログ245を格納している。オペレーティングシステム250は、前記CPU205による処理を制御するものであり、典型的には前記データ記憶装置230に格納されており、(図示例では)前記RAM235にロードされて実行される。セキュリティプ

口

グラム 255 は、入ってくるダウンローダブルの検査を制御するものであり、これも前記データ記憶装置 230 に格納されていて、(図示例では) 前記 RAM 235 にロードされて前記 CPU 205 によって実行されてよい。

図 3 は、前記セキュリティプログラム 255 およびセキュリティデータベース 240 の詳細を示すブロック図である。前記セキュリティプログラム 255 は、ID ジェネレータ 315 と、該 ID ジェネレータ 315 に接続されたポリシーファインダ 317 と、該ポリシーファインダ 317 に接続された第 1 のコンパレータ 320 を含んでいる。前記第 1 のコンパレータ 320 は、4 つの異なる経路、すなわち、経路 1、経路 2、経路 3 および経路 4、を介して論理エンジン 333 に接続されている。前記経路 1 は、前記第 1 のコンパレータ 320 から前記論理エンジン 333 への直接的な接続部を含む。前記経路 2 は、前記第 1 のコンパレータ 320 に接続されたコードスキヤナと、該コードスキヤナ 325 を前記論理エンジン 333 に接続するアクセス・コントロール・リスト (ACL) コンパレータ 330 を含む。前記経路 3 は、前記第 1 のコンパレータ 320 に接続された証明書スキヤナ 340 と、該証明書スキヤナ 340 を前記論理エンジン 333 に接続する証明書コンパレータ 345 を含む。前記経路 4 は、前記第 1 のコンパレータ 320 を前記論理エンジン 333 に接続するユニフォーム・リソース・ロケータ (URL) を含む。また、記録エンジン 335 は、前記論理エンジン 333 と前記イベントログ 245 との間に接続されている。

前記セキュリティプログラム 255 は前記セキュリティデータベース 240 と協働して動作し、該セキュリティデータベース 240 は、セキュリティポリシー 305 と、既知のダウンローダブル 307 と、既知の証明書 309 と、前記既知のダウンローダブル 307 に対応したダウンローダブル・セキュリティ・プロファイル (DSP) 310 を含む。前記セキュリティポリシー 305 は、特定のユーザ 260 に固有のポリシーと、入ってくるダウンローダブルを許可するべきかまたは拒絶するべきかを判定するためのデフォルト (または一般的) ポリシーとを含む。これらのセキュリティポリシー 305 は、拒絶すべき特定のダウンロー

ダブル、許可すべき特定のダウンローダブル、または、未知のダウンローダブルを許可するために必要な規準を指示することができる。図4において、前記セキュリティポリシー305は、ポリシーセレクタ405と、アクセスコントロールリスト410と、信頼性が確認された証明書リスト415と、URLルールベース420と、管理オーバライドごとに許可または拒絶すべきダウンローダブルのリスト425とを含む。

前記既知のダウンローダブル307は、オリジナル機器マニュファクチャラ（OEM）が悪意あるものとして認識しているダウンローダブルのリスト、および、このセキュリティプログラム255によって前に受け取られたダウンローダブルのリストを含む。前記DSPデータ310は、各前記既知のダウンローダブル307によって試みられる可能性のあるすべての潜在的に悪意のあるまたは疑わしいコンピュータオペレーションのリストを含むものであり、さらに、これらのそれぞれの引き数を含んでいてよい。オペレーションの確認された引き数は“確定された引き数”と称され、確認されていない引き数は“確定されていない引き数”と称される。次に、前記コードスキヤナ325に関連して、前記DSPデータ310について説明する。

前記IDジェネレータ315は、前記外部通信インターフェイス210を介して前記内部通信インターフェイス105からダウンローダブル（その送り元のURLおよび意図された受領者のユーザIDを含む）を受け取り、各ダウンローダブルを識別するためのダウンローダブルIDを生成する。該ダウンローダブルIDは、完全なダウンローダブルコードのデジタル・ハッシュ（hash）を含むのが好ましい。また、前記IDジェネレータ315は、ダウンローダブルIDの生成のためのコードに含まれまたはこれによって識別されるすべての構成要素を前もってフェッチするのが好ましい。例えば、該IDジェネレータ315は、ダウンローダブルIDの生成のためのJava（商標）アブレットのバイトコードに含まれまたはこれによって識別されるすべてのクラスを前もってフェッチしてよい。同様に、該IDジェネレータ315は、ActiveX（商標）コントロールがダウンローダブルIDを算出するためのINFFファイルにリストされたすべての構成要

素を取り出してよい。従って、ダウンローダブルのダウンローダブル I D は、前記 I D ジェネレータ 315 が同一のダウンローダブルを受け取る時は常に同じものとなる。前記 I D ジェネレータ 315 は、生成されたダウンローダブル I D を

前記既知のダウンローダブル 307 のリストに加える（それが未だリストされていない場合）。そして、前記 I D ジェネレータ 315 は、前記ダウンローダブルおよびダウンローダブル I D を前記ポリシーファインダ 317 に送る。

前記ポリシーファインダ 317 は、意図されたユーザのユーザ I D およびダウンローダブル I D を使用して、受け取ったダウンローダブルに適用される特定のセキュリティポリシー 305 を選択する。前記ユーザ（またはそのスーパーグループの 1 つ）および前記ダウンローダブルについて定義された特定のポリシー 305 が存在する場合、そのポリシーが選択される。そうでない場合、前記ユーザ（またはそのスーパーグループの 1 つ）について定義された一般的なポリシー 305 が選択される。こうして、前記ポリシーファインダ 317 は、選択した前記ポリシーを前記第 1 のコンパレータ 320 に送る。

前記第 1 のコンパレータ 320 は、前記ポリシーファインダ 317 から、前記ダウンローダブル、ダウンローダブル I D およびセキュリティポリシー 305 を受け取る。前記第 1 のコンパレータ 320 は、前記セキュリティポリシー 305 を検査し、前記ダウンローダブルを許可するためにどのステップが必要であるかを判定する。例えば、前記セキュリティポリシー 305 は、このダウンローダブルを許可するために、前記経路 1、経路 2、経路 3 および経路 4 からなる 4 つの経路のすべてを通らなければならない、ということを示してよい。代案として、前記セキュリティポリシー 305 は、このダウンローダブルを許可するために、前記経路のうちの 1 つだけを通らなければならない、ということを指示してよい。前記第 1 のコンパレータ 320 は、前記セキュリティポリシー 305 によって示された経路に適当な情報を送ることによって、これに応答する。

#### 経路 1

経路 1において、前記第 1 のコンパレータ 320 は、前記ポリシーファインダ 317 から受け取ったセキュリティポリシー 305 のポリシーセレクタ 405 を

チェックする。該ポリシーセレクタ405が“許可された”または“拒絶された”ものである場合、前記第1のコンパレータ320は、この結果を直接前記論理エンジン333に送る。そうでない場合、前記第1のコンパレータ320は、ポリシーセレクタ405の内容に基づいて、経路2および／または経路3および／また

たは経路4での比較を行う。なお、前記第1のコンパレータ320それ自体は、前記ダウローダブルIDを、管理オーバライド425ごとに許可または拒絶するためのダウローダブルのリストと比較する。すなわち、システムセキュリティアドミニストレータは、特定のダウローダブルを“許可されるもの”または“拒絶されるもの”として定義することができる。

代案として、前記論理エンジン333が、各前記経路の結果を受け取り、前記ポリシーセレクタ405に基づき、前記ダウローダブルを許可すべきか、または拒絶すべきかを最終的に判定するようにしてもよい。前記第1のコンパレータ320は、その比較結果を前記論理エンジン333に通知する。

#### 経路2

経路2において、前記第1のコンパレータ320は、前記ダウローダブル、ダウローダブルIDおよびセキュリティポリシー305を前記コードスキナ325に送る。前記受け取ったダウローダブルのDSPデータ310が既知のものである場合、前記コードスキナ325は、その情報を読み出し、前記ACLコンパレータ330に送る。そうでない場合、前記コードスキナ325は前記DSPデータ310を分解する。すなわち、前記コードスキナ325は、通常の解析技術を使用して、前記ダウローダブルのコード（予めフェッチされたすべての構成要素を含む）をDSPデータ310に分解する。該DSPデータ310は、特定のダウローダブル307によって試みられる可能性のあるすべての潜在的に悪意のあるまたは疑わしいコンピュータオペレーションのリストを含むものであり、さらに、これらのオペレーションの各々の引き数を含んでよい。例えば、DSPデータ310は、特定のファイルからのREAD、未分解のホストへのSEND等を含んでいてよい。前記コードスキナ325は、今まで潜在的に悪意

のあるものと判断され得たダウンローダブルコードにおけるすべてのオペレーションのリスト、および、前記ダウンローダブルコードによってアクセスされるすべてのファイルのリストとして前記D S Pデータ310を生成することができる。なお、前記コードスキャナ325は、前記コードにおける、望ましくないまたは該コードがハッカによって書かれたことを示唆するパターンをサーチすることができる。

潜在的に悪意のあるものとして判断されるオペレーションのリストの例

ファイルオペレーション：ファイルのREAD（読み出し）、ファイルのWRITE（書き込み）；

ネットワークオペレーション：ソケットによるLISTEN（聞き取り）、ソケットへのCONNECT（接続）、データのSEND（送出）、データのRECEIVE（受取り）、VIEW INTRANET（インターネット視察）；

登録オペレーション：登録アイテムのREAD（読み出し）、登録アイテムのWRITE（書き込み）；

オペレーティングシステムオペレーション：EXIT WINDOW（ウィンドウ退出）、EXIT BROWSER（ブラウザ退出）、START PROCESS/THREAD（オペレーション／スレッドの開始）、KILL PROCESS/THREAD（オペレーション／スレッドの停止）、CHANGE PROCESS/THREAD PRIORITY（オペレーション／スレッドの優先順位の変更）、DYNAMICALLY LOAD A CLASS/LIBRARY（クラス／ライブラリの動的ロード）など；

資源使用しきい値：メモリ、CPU、グラフフィックスなど。

好ましい実施の形態において、前記コードスキャナ325は全内容検査を実行する。しかしながら、セキュリティの低減を伴うが速度を高める目的で、前記コードスキャナ325は、前記ダウンローダブルのヘッダのような一部分のみを検査してもよい。そして、該コードスキャナ325は、そのD S Pデータを（そのダウンローダブルIDに対応する）D S Pデータ310に格納し、前記セキュリティポリシー305との比較のために、前記ダウンローダブルおよびD S Pデータを前記A C Lコンパレータ330に送る。

該A C Lコンパレータ330は、前記コードスキャナ325から前記ダウンロ

ーダブル、これに対応するD S Pデータおよびセキュリティポリシー3 0 5を受け取り、前記D S Pデータをセキュリティポリシー3 0 5と比較する。すなわち、前記A C Lコンパレータ3 3 0は、受け取ったダウンローダブルのD S Pデータを、受け取ったセキュリティポリシー3 0 5におけるアクセスコントロールリスト4 1 0と比較する。該アクセスコントロールリスト4 1 0は、前記ダウンローダブルを通すべきか、または、阻止すべきかを示す規準を含む。例えば、ア

クセスコントロールリストは、前記D S PデータがシステムファイルへのWRITEコマンドを含む場合に該ダウンローダブルが阻止されるべきものと示してよい。前記A C Lコンパレータ3 3 0は、その結果を前記論理エンジン3 3 3に送る。

#### 経路3

経路3において、前記証明書スキャナ3 4 0は、前記受け取ったダウンローダブルがVerisign, Inc.のような証明書発行者によって署名されているか否かを判定し、該ダウンローダブルに含まれる証明書をスキャンする。前記証明書スキャナ3 4 0は、検出された証明書を前記証明書コンパレータ3 4 5に送る。該証明書コンパレータ3 4 5は、セキュリティアドミニスターによって信頼できるものと判断された既知の証明書を読み出し、前記検出された証明書を該既知の証明書と比較し、前記ダウンローダブルが信頼性のおける証明書によって署名されたものか否かを判定する。該証明書コンパレータ3 4 5は、その結果を前記論理エンジン3 3 3に送る。

#### 経路4

経路4において、前記U R Lコンパレータ3 5 0は、前記ダウンローダブルのソースを示すU R LをU R Lルールベース4 2 0に格納されたU R Lに対して検査し、前記ダウンローダブルが信頼性のおけるソースから送られたものか否かを判定する。前記セキュリティポリシー3 0 5に基づき、前記U R Lコンパレータ3 5 0は、前記ダウンローダブルが信頼のおけないソースから送られたもの、すなわち、信頼のおけるソースから送られたものではない場合に、該ダウンローダブルを疑わしいものと判断してよい。例えば、前記ダウンローダブルが既知のハッカから送られたものである場合、該ダウンローダブルは、疑わしいものと判断

され、悪意のあるものと推定されてよい。前記UR Lコンパレータ350は、その結果を前記論理エンジン333に送る。

前記論理エンジン333は、各前記経路の結果および前記セキュリティポリシー305におけるポリシーセレクタ405を検査し、前記ダウンローダブルを許可すべき、または、拒絶すべきかを判定する。前記ポリシーセレクタ405は、各前記経路から受け取った論理表現を含む。例えば、該ダウンローダブルが前記経路のうちのいずれかで阻止された場合、すなわち、該ダウンローダブルが悪意

のあるものである場合（経路1）、該ダウンローダブルが疑わしいオペレーションを要求する可能性のあるものである場合（経路2）、該ダウンローダブルが信頼性が確認された証明書発行者によって署名されていないものである場合（経路3）、または、該ダウンローダブルが信頼のおけないソースから送られたものである場合（経路4）に、前記論理エンジン333はこのダウンローダブルを拒絶することができる。前記論理エンジン333は、前記セキュリティポリシー305に含まれるポリシーセレクタ405に従って、他の論理表現を適用してよい。

前記ダウンローダブルが通過可能であると前記ポリシーセレクタ405が示す場合、前記論理エンジン333は、該ダウンローダブルを意図された受領者に送る。前記ダウンローダブルが拒絶すべきものと前記ポリシーセレクタ405が示す場合、前記論理エンジン333は、悪意のないダウンローダブルを意図された受領者に送り、これにより、前記内部ネットワークセキュリティシステム110が前記オリジナルのダウンローダブルを放棄した旨ユーザに通知する。さらに、前記論理エンジン333は前記記録エンジン335にステータスレポートを送り、該記録エンジン335は、例えばMISディレクタによるその後の再検査のために、前記レポートをデータ記憶装置230のイベントログ245に格納する。

図5はセキュリティ管理コンソール120の詳細を示すブロック図であり、該セキュリティ管理コンソール120は、前記通信チャネル135に接続されたセキュリティポリシーエディタ505と、前記通信チャネル135とユーザ通知エンジン515との間に接続されたイベントログ分析エンジン510と、前記通信チャネル135に接続されたダウンローダブルデータベース検査エンジン

520とを具備している。さらに、前記セキュリティ管理コンソール120は、図2に示されたコンピュータ構成要素と同様なコンピュータ構成要素を備えている。

前記セキュリティポリシーエディタ505は、I/Oインターフェイス215と同様なI/Oインターフェイスを使用して、前記セキュリティポリシー305の許可されたユーザ修正を可能にする。すなわち、前記セキュリティポリシーエディタ505は、許可されたユーザが、ユーザ260に対応する特定のセキュリティポリシー305、デフォルトまたは一般的なセキュリティポリシー305、

管理オーバライドごとに拒絶すべきダウンローダブル、管理オーバライドごとに許可すべきダウンローダブル、信頼性が確認された証明書のリスト415、ポリシーセレクタ405、アクセスコントロールリスト410、URLルールベース420におけるURLなどを修正することを可能にする。例えば、許可されたユーザが新たな悪意のあるダウンローダブルについて知った場合、該ユーザは、システムオーバライドごとに拒絶すべきダウンローダブルに前記ダウンローダブルを加えることができる。

前記イベントログ分析エンジン510は、前記データ記憶装置230に格納されたイベントログ245に含まれるステータスレポートを検査する。該イベントログ分析エンジン510は、(例えば、セキュリティシステムマネージャまたはMISディレクタなどの)ユーザの通知が許可されたものか否かを判定する。例えば、30分の期間内に内部ネットワークセキュリティシステム110によって10個の疑わしいダウンローダブルが放棄された場合、前記イベントログ分析エンジン510は、ユーザ通知を許可し、これにより、潜在的な切迫したセキュリティ上の脅威を示してよい。従って、前記イベントログ分析エンジン510は、ユーザ通知エンジン515に対してユーザに通知するよう指示する。該ユーザ通知エンジン515は、内部通信インターフェイス220または外部通信インターフェイス210を介して、前記ユーザにeメールを送つてよく、または、前記ユーザのディスプレイ装置(図示せず)にメッセージを表示してよい。

図6Aは、疑わしいダウンローダブルから内部コンピュータネットワーク11

5を保護するための方法600を示すである。該方法600は、前記IDダウンローダブル315がダウンローダブルを受け取るステップ602から始まる。前記IDダウンローダブル315は、ステップ604において、好ましくは、(予めフェッチされた構成要素を含む)ダウンローダブルコードのデジタルハッシュを生成することによって、受け取ったダウンローダブルを示すダウンローダブルIDを生成する。ステップ606において、前記ポリシーファインダ317は、意図された受領者(または、該意図された受領者が属するグループ)を示すユーザIDおよびダウンローダブルに対応する適当なセキュリティポリシー305を検出する。この選択されるセキュリティポリシー305は、デフォルトセキュリ

ティポリシー305であつてよい。次に、図6Bを参照して、ステップ606についてより詳細に説明する。

ステップ608において、前記第1のコンパレータ320は、管理オーバライド425ごとに許可または拒絶すべきダウンローダブルのリストを入ってくるダウンローダブルのダウンローダブルIDに対して検査し、該ダウンローダブルを自動的に許可すべきか否かを判定する。許可すべき場合、ステップ612において、前記第1のコンパレータ320は、その結果を前記論理エンジン333に送る。許可すべきでない場合、前記方法600はステップ610に進む。ステップ610において、前記第1のコンパレータ320は、管理オーバライド425ごとに拒絶すべきダウンローダブルのリストを入ってくるダウンローダブルのダウンローダブルIDに対して検査し、該ダウンローダブルを自動的に拒絶すべきか否かを判定する。拒絶すべき場合、ステップ612において、前記第1のコンパレータ420は、その結果を前記論理エンジン333に送る。拒絶すべきでない場合、前記方法600はステップ614に進む。

ステップ614において、前記第1のコンパレータ320は、前記ダウンローダブルが経路4に従ってテストされるべき旨前記セキュリティポリシー305によって示されているか否かを判定する。NOである場合、前記方法600はステップ618にジャンプする。YESである場合、前記URLコンパレータ350

は、ステップ 616において、前記入ってくるダウンローダブルに含まれたUR Lを前記URLルールベース420と比較し、そして、前記方法600はステップ618に進む。

ステップ618において、前記第1のコンパレータ320は、前記ダウンローダブルが経路2に従ってテストされるべき旨前記セキュリティポリシー305によって示されているか否かを判定する。NOである場合、前記方法600はステップ620にジャンプする。YESである場合、ステップ626において、前記コードスキヤナ235は、前記入ってくるダウンローダブルのダウンローダブルIDに基づいてDSPデータ310を検査し、該ダウンローダブルが予め分解されたものか否かを判定する。YESである場合、前記方法600はステップ630にジャンプする。そうでなければ、ステップ628において、前記コードスキ

ヤナ235は、前記ダウンローダブルをDSPデータに分解する。ダウンローダブル分解は図7を参照してより詳細に説明される。ステップ630では、ACLコンパレータ330が、入ってくるダウンローダブルのDSPデータを、アクセスコントロールリスト410（これはダウンローダブルがテストに通るか落ちるかに必要な基準を含む）に対して比較する。

ステップ620において、前記第1のコンパレータ320は、前記ダウンローダブルが前記経路3に従ってテストされるべき旨前記セキュリティポリシー305によって示されているか否かを判定する。NOである場合、前記方法600は、ステップ612に戻り、実行された各テストの結果を前記論理エンジン333に送る。YESである場合、ステップ622において、前記証明書スキヤナ622は、前記ダウンローダブルをスキャンし、そこに含まれる証明書をスキャンする。ステップ624において、前記証明書コンパレータ345は、信頼性が確認された証明書リスト(TCL)415から信頼性が確認された証明書を読み出し、前記ダウンローダブルに含まれる証明書を前記信頼性が確認された証明書と比較し、前記ダウンローダブルが信頼性が確認されたソースによって署名されたものであるか否かを判定する。そして、前記証明書コンパレータ345が各前記経路の結果を前記論理エンジン333に送ることによって、前記方法600はステ

ップ612に進む。前記論理エンジン333のオペレーションについて、図6Cを参照して以下に詳しく説明する。そして、前記方法600は終了する。

当業者に認識され得るよう、前記テストは様々異なる順序で実行されてよく、各前記テストが実行されなくてもよい。さらに、当業者に認識され得るよう、前記経路1は図6Aにおいて自動許可または拒絶オペレーションとして説明したが、該経路1の結果は前記論理エンジン333によって適用される他の述語であってもよい。さらに、前記テストは図6Aにおいて直列的に示されているが、これらのテストは図3に示したように並列的に実行されてもよい。

図6Bは、図6Aのステップ606（以下、方法606という）の詳細を示すフローチャートである。この方法606によると、先ずステップ650において、前記ポリシーファインダ317は、前記セキュリティポリシー305がユーザIDおよびダウンローダブルに対応する特定のセキュリティポリシーを含むか否か

を判定する。YESである場合、前記ポリシーファインダ317は、ステップ654において、前記対応するセキュリティポリシー305をフェッチする。NOである場合、前記ポリシーファインダ317は、ステップ652において、前記ユーザIDに対応するデフォルトまたは一般的セキュリティポリシー305をフェッチする。そして、前記方法606が終了する。

図6Cは、前記入ってくるダウンローダブルを許可すべきか拒絶すべきかを判定するための方法655の詳細を示すフローチャートである。この方法655によると、先ずステップ660において、前記論理エンジン333は、前記第1のコンパレータ320、ACLコンパレータ330、証明書コンパレータ345およびURLコンパレータ350からそれぞれの結果を受け取る。前記論理エンジン333は、ステップ662において、前記結果を前記セキュリティポリシー305に含まれるポリシーセレクタ405と比較し、ステップ664において、前記ポリシーセレクタ405がダウンローダブルの通過を確認するか否かを判定する。例えば、前記ダウンローダブルが経路1～4のテストのうちの1つを通過する場合、前記論理エンジン333が該ダウンローダブルを通す旨前記ポリシーセ

レクタ405によって示されてよい。前記ダウンローダブルが通過すべき旨前記ポリシーセレクタ405が示す場合、前記論理エンジン333は、ステップ666において、前記ダウンローダブルを意図された受領者に送る。ステップ668において、前記論理エンジン333はその結果を前記記録エンジン335に送り、該記録エンジン335は、その後の再検査のために前記結果を前記イベントログ245に格納する。そして、方法655が終了する。ステップ644において前記ダウンローダブルが通過すべきでない旨前記ポリシーセレクタ405が示した場合、前記論理エンジン333は、ステップ670において前記ダウンローダブルを停止させ、そしてステップ672において、前記入ってくるダウンローダブルが阻止されたことをユーザに知らせるために悪意のない代替ダウンローダブルを送る。

図7は、ダウンローダブルをDSPデータ310に分解するための図6Aのステップ628（以下、方法628という）の詳細を示すフローチャートである。この方法628によると、先ずステップ705において、前記コードスキャナ3

25は前記ダウンローダブルのマシンコードをディアセンブルする。前記コードスキャナ325は、ステップ710において前記マシンコードにおけるそれぞれのコマンドを分解し、ステップ715において、前記分解されたコマンドが疑わしいものか否か（すなわち、前記コマンドが図3を参照して上述したリストに示されたオペレーションのうちの1つか否か）を判定する。NOである場合、ステップ725において、前記コードスキャナ325は、前記ダウンローダブルの分解を完了したか否か、すなわち、前記ダウンローダブルコードにおけるすべてのオペレーションが分解されたか否かを判定する。YESである場合、この方法628が終了する。NOの場合、この方法628はステップ710に戻る。

前記コードスキャナ325は、ステップ715において前記分解された構成要素が疑わしいものであると判定した場合、ステップ720において前記疑わしいコマンドおよびそのコマンドパラメータをデコードして、DSPデータとして登録する。ステップ720において、前記コードスキャナ325は、前記コマンドおよびコマンドパラメータをコマンドクラス（例えば、ファイルオペレーション

、ネットワークオペレーション、登録オペレーション、オペレーティングシステムオペレーション、資源使用しきい値)に基づくフォーマットで登録する。そして、この方法628はステップ725にジャンプする。

図8は、ダウンローダブルを識別するためのダウンローダブルIDを生成するための方法800を示すフローチャートである。該方法800によると、先ずステップ810において、前記IDジェネレータ315は、前記外部通信ネットワーク105からダウンローダブルを受け取る。前記IDジェネレータ315は、ステップ820において、前記ダウンローダブルコードにおいて参照される構成要素のいくつかまたはすべてをフェッチしてよく、ステップ830において該フェッチされた構成要素を前記ダウンローダブルコードに含ませる。ステップ840において、前記IDジェネレータ315は、前記ダウンローダブルコードの少なくとも一部についてハッシングファンクション(hashing function; ハッシュ関数)を実行することにより、ダウンローダブルIDを生成する。ステップ850において、前記IDジェネレータ315は、生成された前記ダウンローダブルIDをDSPデータ310に対する参照としてセキュリティデータベース24

0に格納する。従って、前記ダウンローダブルIDは、同一のダウンローダブルに遭遇するごとに同じものとなる。

この発明は、上述の好ましい実施の形態に限定されることなく、様々な変更が可能である。例えば、この発明は内部コンピュータネットワークを保護するためのシステムとして説明したが、この発明は、個々のコンピュータを保護するためのシステムとして実施してもよい。また、この発明の構成要素は、プログラム化された汎用のディジタルコンピュータを使用して、アプリケーションごとに固有の集積回路を使用して、または、相互接続された通常の構成要素および回路を使用して実現されてよい。ここで述べた実施例は、あくまでも説明の為のものであって、完全さや限定を意図しているものではない。多くの別形態と変形とが、前述の教示に照らして、可能である。

【図1】

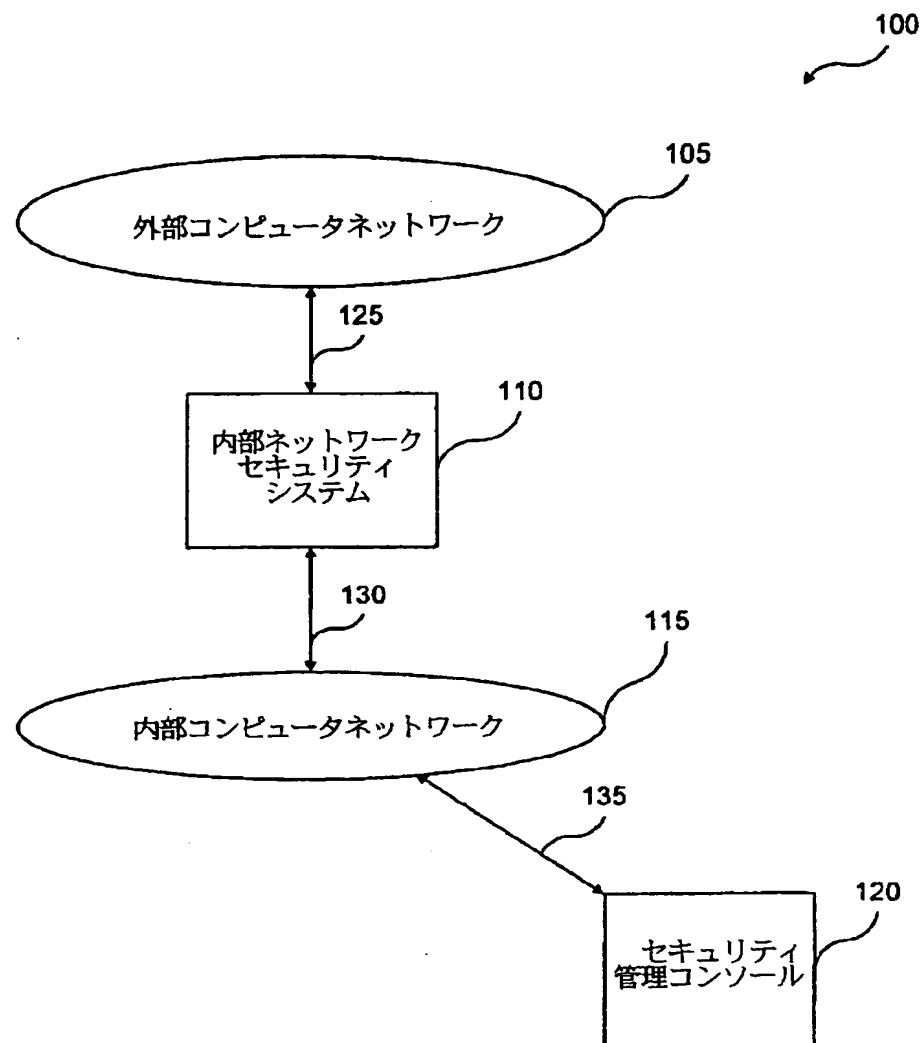
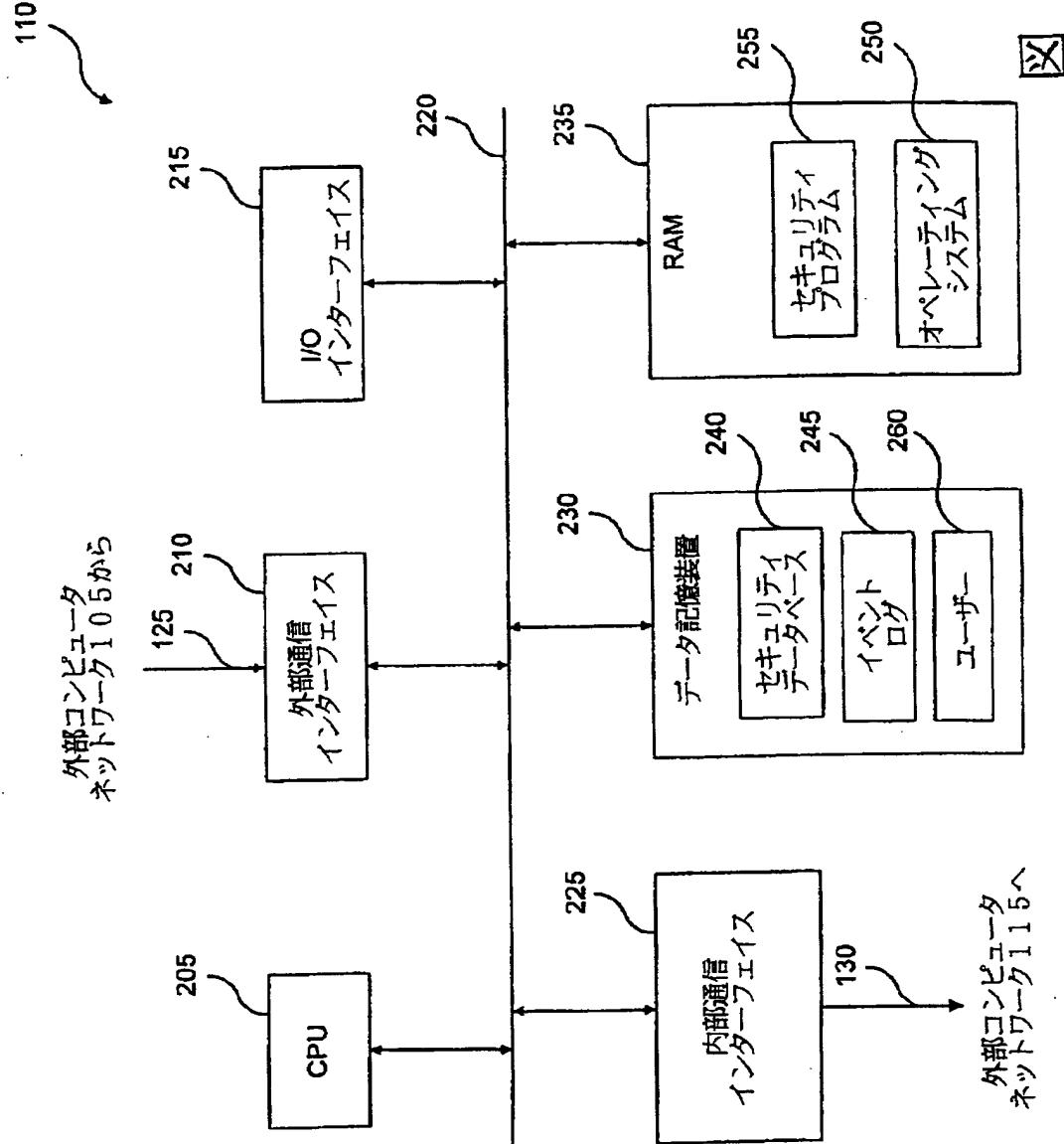
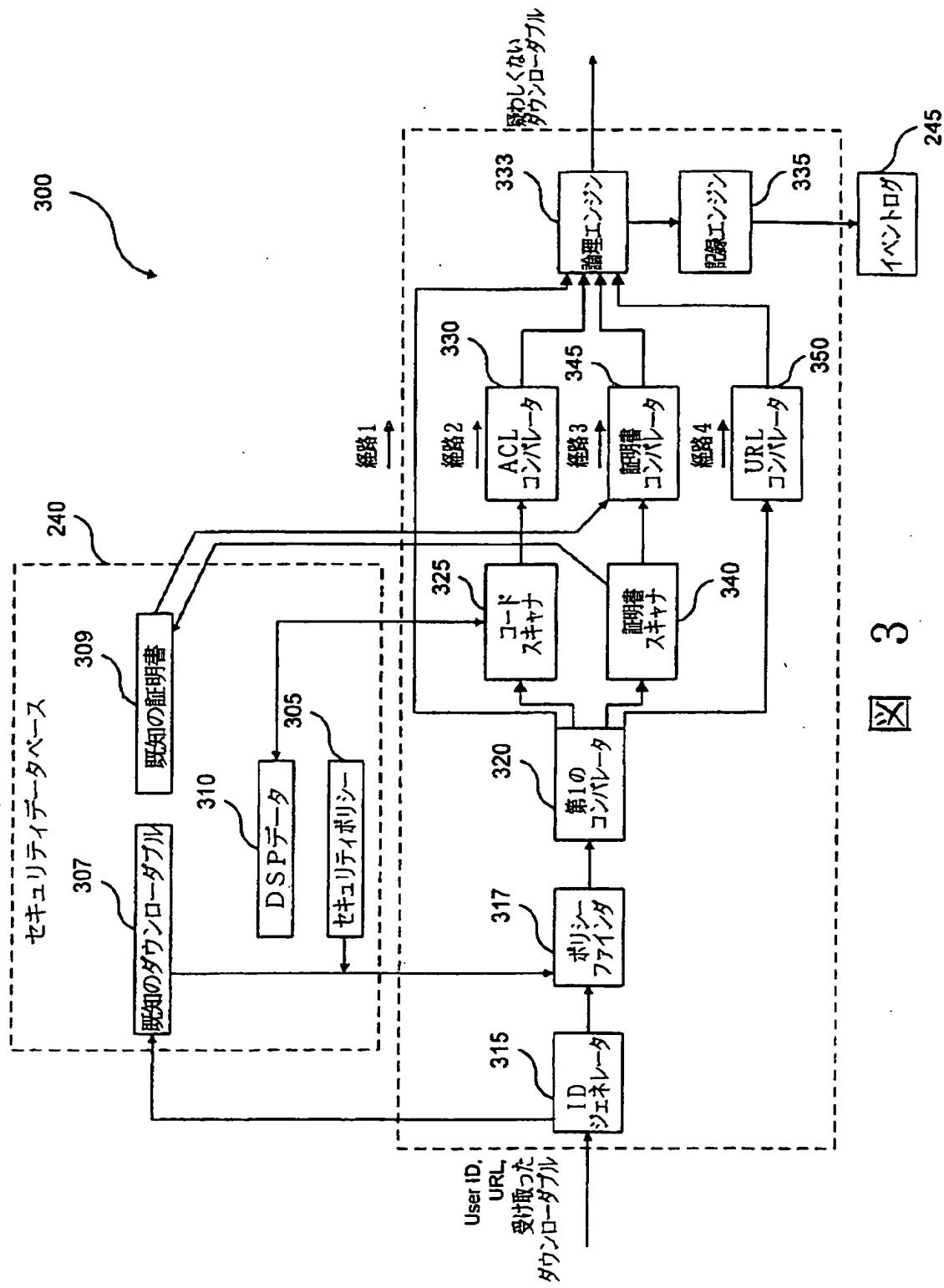


図 1

【図2】



[☒ 3 ]



【図4】

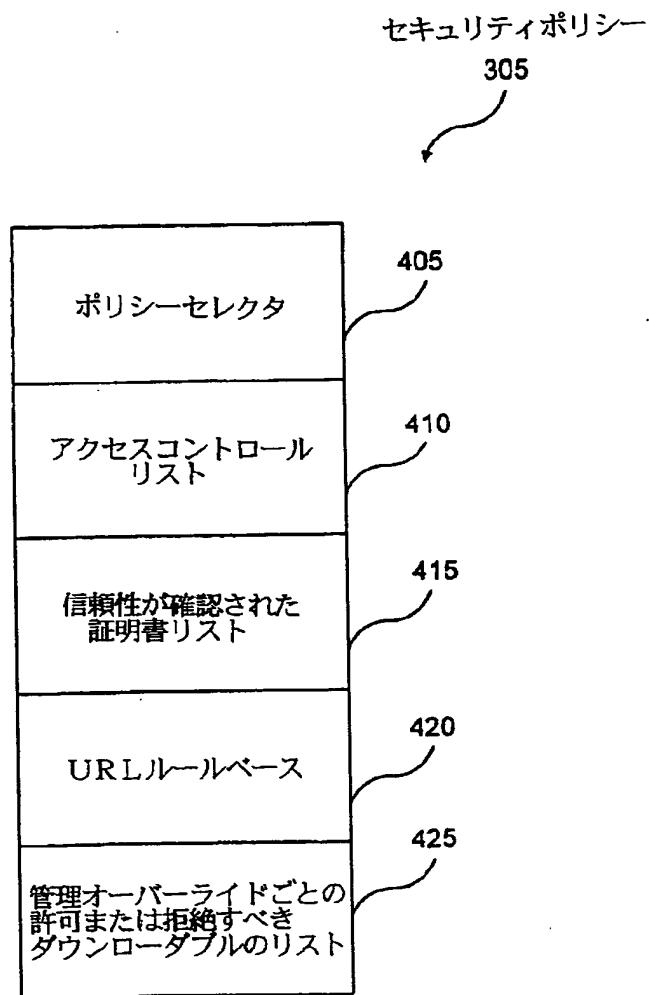


図 4

【図5】

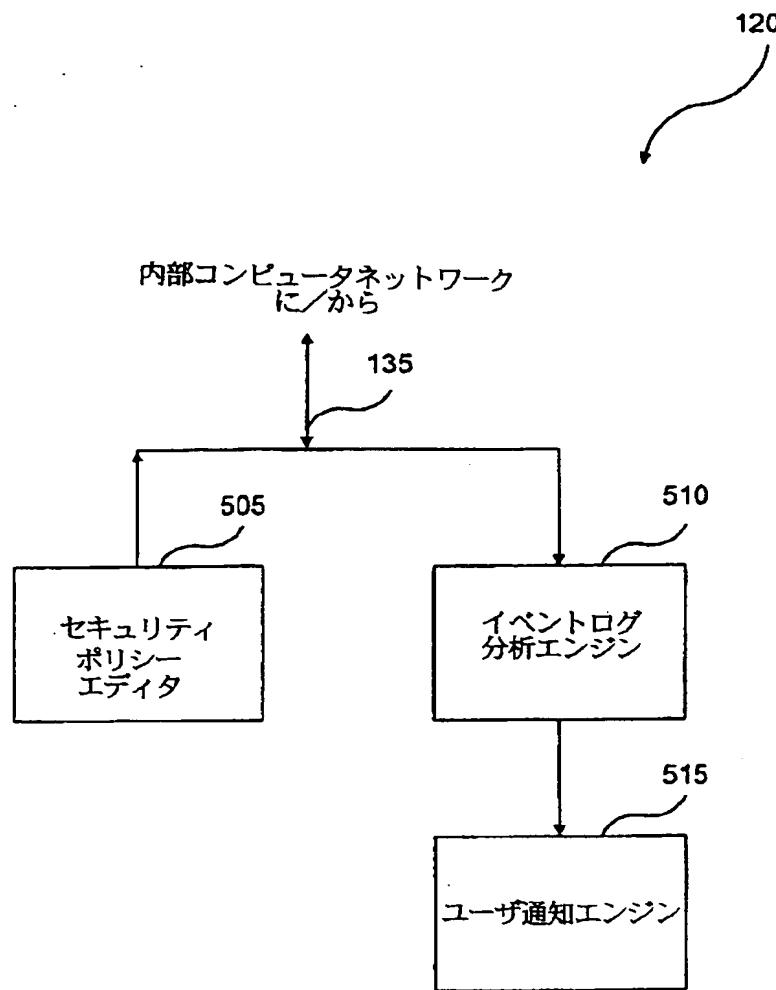


図 5

【図6】

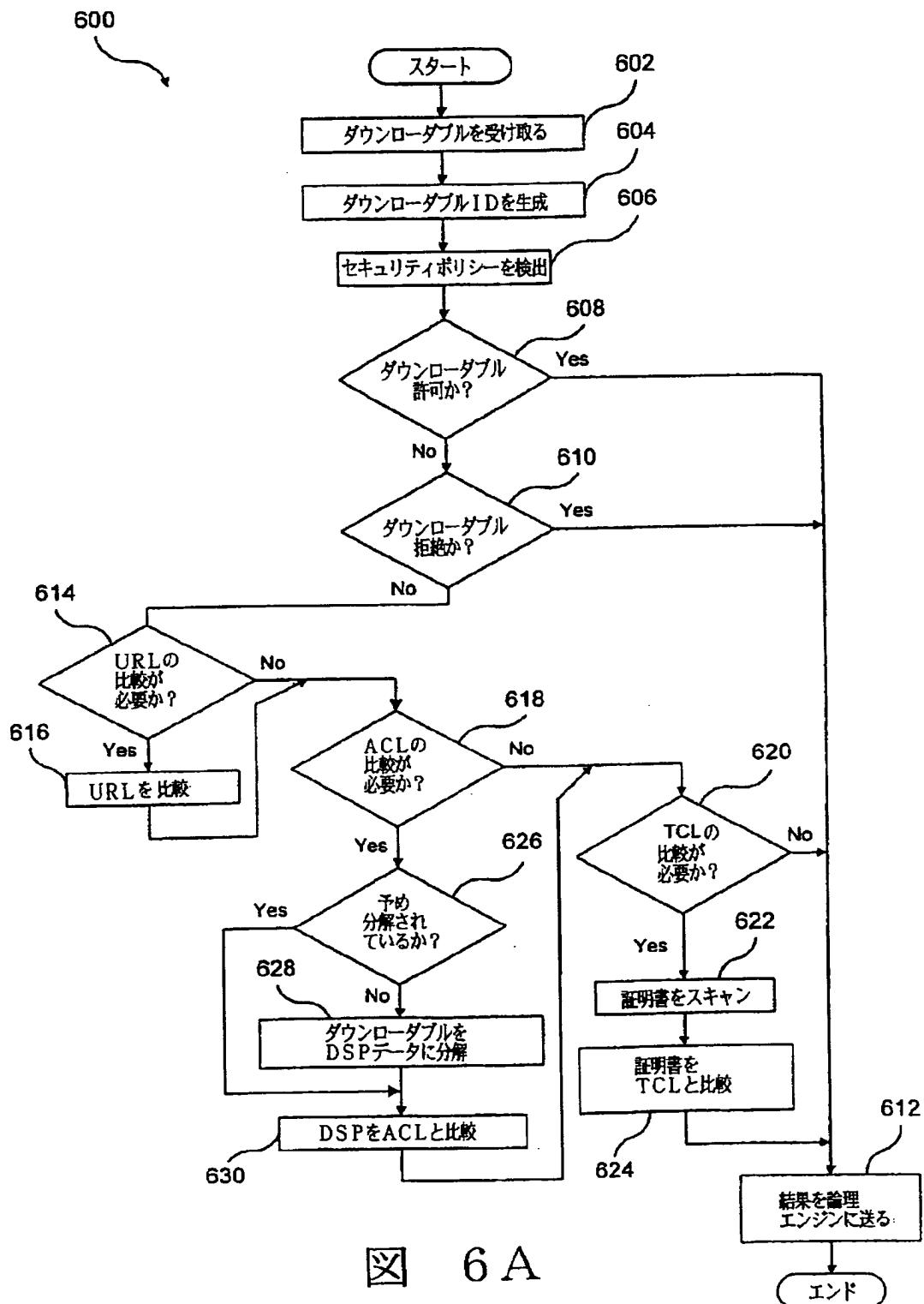


図 6 A

【図6】

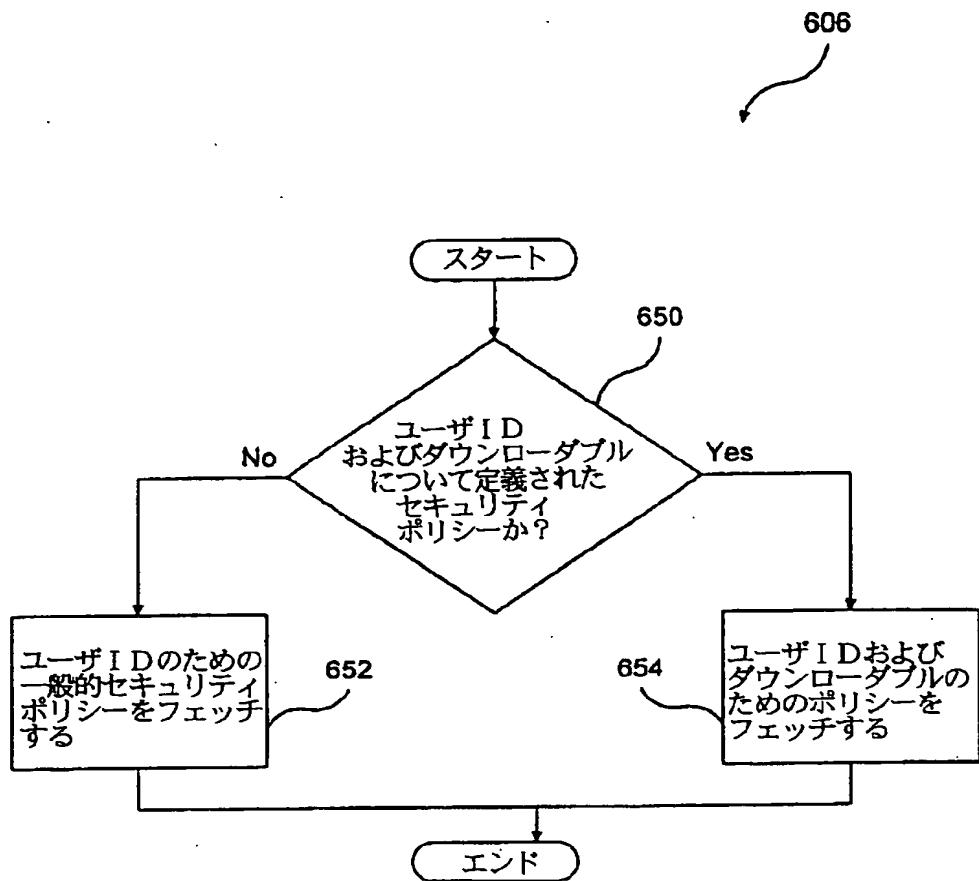


図 6B

【図6】

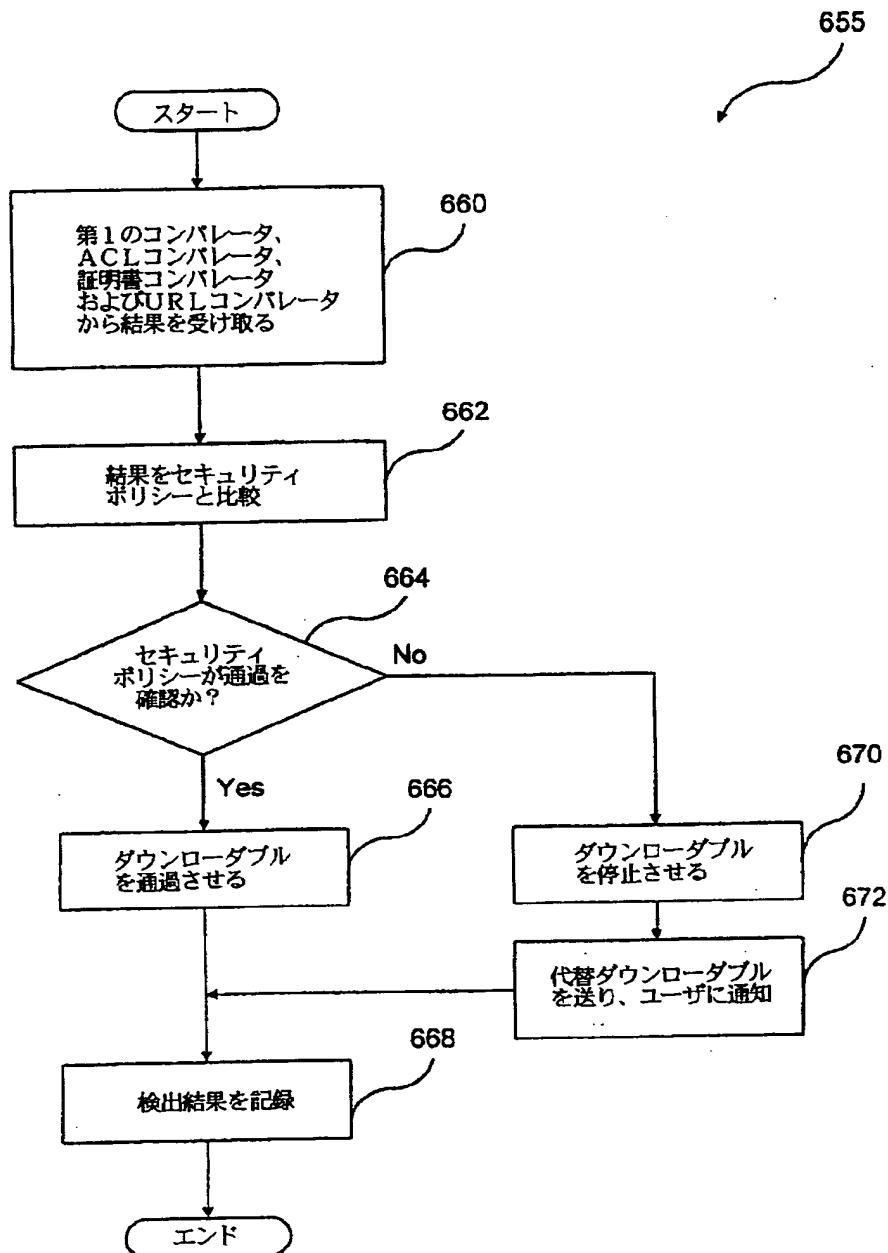


図 6C

【図7】

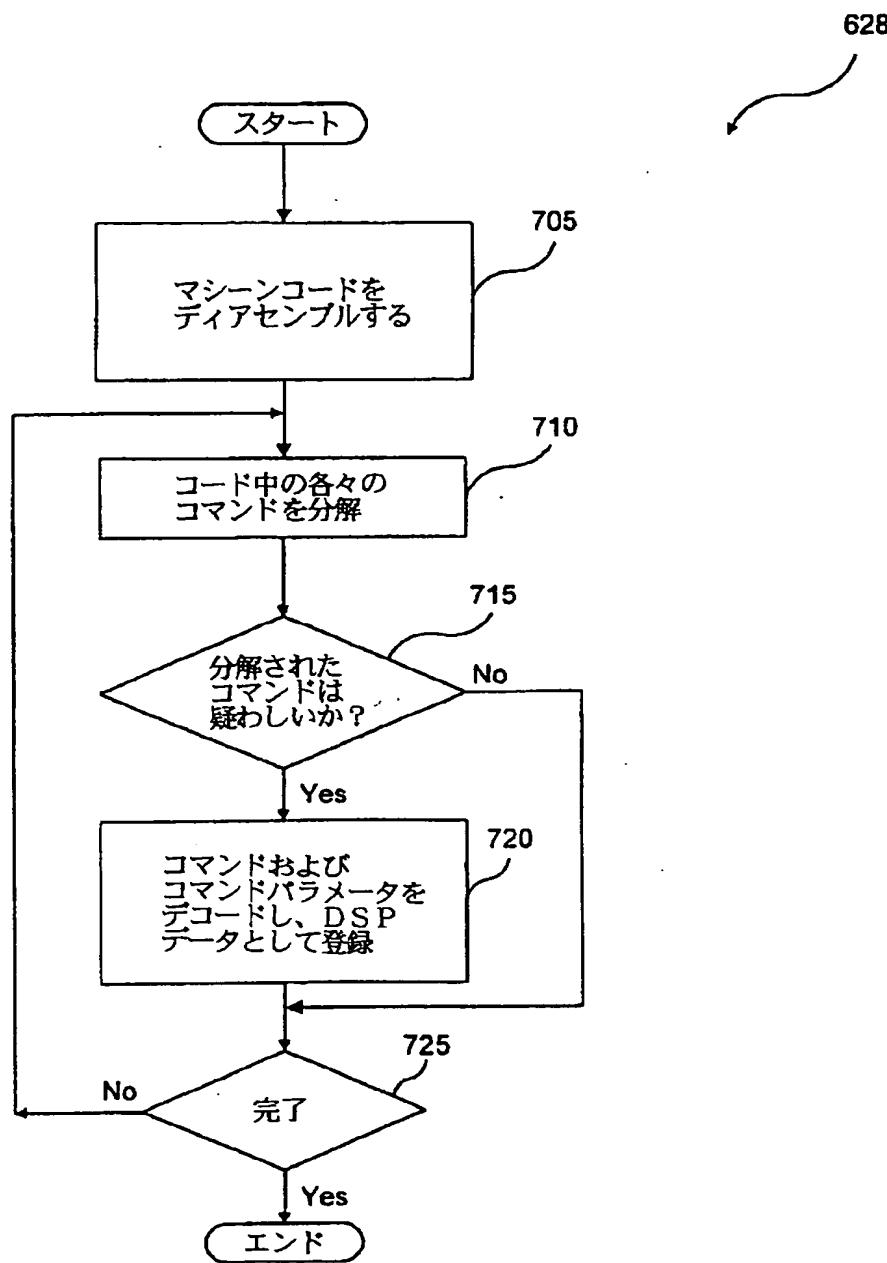


図 7

【図8】

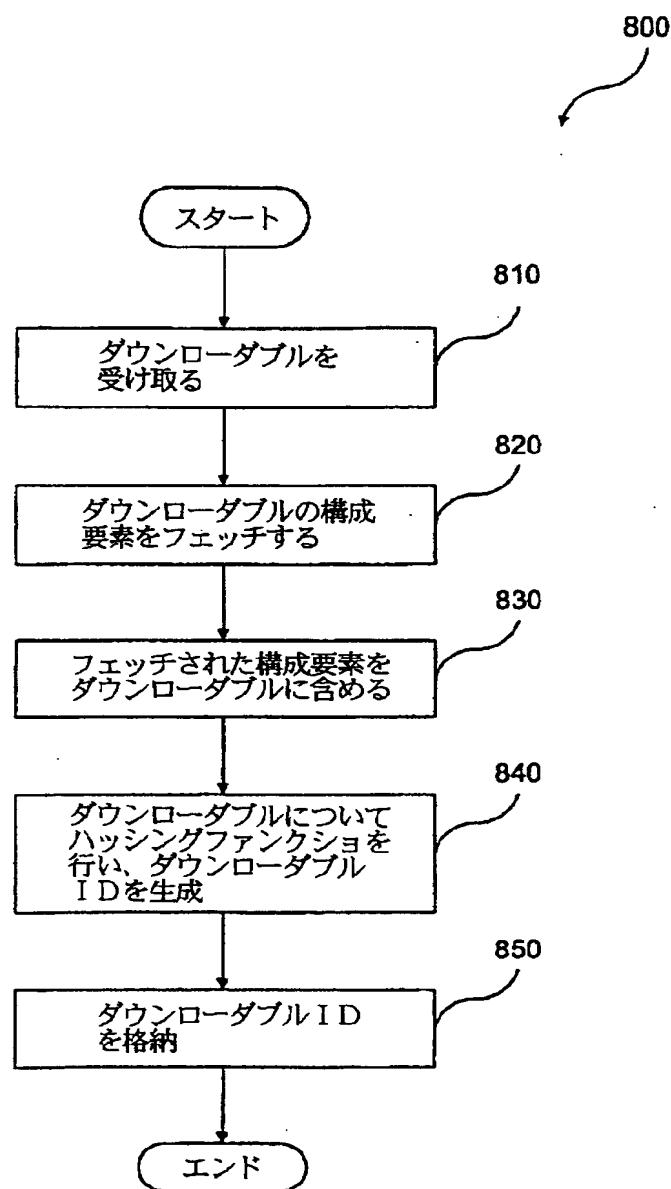


図 8

【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB97/01626

<b>A. CLASSIFICATION OF SUBJECT MATTER</b>		
IPC(6) : G06F 19/00, 15/12, 9/44 US CL : 395/187.01, 186, 188.01, 200.48, 200.59, 10 According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b>		
Minimum documentation searched (classification system followed by classification symbols)  U.S. : 395/187.01, 186, 188.01, 200.48, 200.59, 10		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  NONE		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  NONE		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X.P	US 5,572,643 A (JUDSON) 05 November 1996, col. 2, lines 12-53, col. 3, lines 48-67, col. 4, lines 5-51, col. 7, lines 1-13	1-70
X	US 5,077,677 A (MURPHY ET AL) 31 December 1991, COL. 2, LINES 60-66, COL. 19, LINES 8-16	10, 35
X,E	US 5,692,047 A (MCMANIS) 25 November 1997, col. 3, lines 14-29.	66

Further documents are listed in the continuation of Box C.  See patent family annex.

* Special categories of cited documents:	"T"	later documents published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
*A* document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
*B* earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
*L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another invention or other special reasons (as specified)	"A"	document member of the same patent family
*O* document referring to an oral disclosure, use, exhibition or other means		
*P* document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search  25 MARCH 1998	Date of mailing of the international search report  14 MAY 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer  PIERRE EDDY ELISCA <i>John Hall</i> Telephone No. (703) 305-3987

## フロントページの続き

(81) 指定国 E P (A T, B E, C H, D E,  
D K, E S, F I, F R, G B, G R, I E, I T, L  
U, M C, N L, P T, S E), C A, I L, J P

## 【要約の続き】

構成要素を含むダウンローダブルについてのハッシング  
関数を実行することによって、前記ダウンローダブルを  
識別するダウンローダブルIDを算出するためのIDジ  
ェネレータを使用する。前記セキュリティポリシーは、  
(1) 既知の悪意のあるダウンローダブルおよび悪意の  
無いダウンローダブルとの比較、(2) 管理オーバーラ  
イドごとの拒絶または許可すべきダウンローダブルとの  
比較、(3) ダウンローダブルセキュリティプロファイ  
ルデータの、アクセスコントロールリストに対する比  
較、(4) 前記ダウンローダブルに含まれる証明書の、  
信頼性が確認された証明書との比較、(5) 前記ダウン  
ローダブルの送り元のURLの、信頼性が確認されたU  
RLおよび信頼性が確認されていないURLに対する比  
較を含むいくつかの実行すべきテストを指示するもので  
あってよい。これらのテストに基づき、論理エンジン  
は、前記ダウンローダブルを許可または拒絶すべきこと  
を判定することができる。